UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/859,429	05/18/2001	Makoto Kayashima	566.39530VX1	5340

20457 7590 11/16/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 11/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/859,429	KAYASHIMA ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/18/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *18 May 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/761,742.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/8-17-2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

PART III Detailed Action

Drawings

The drawings are objected to under 37 CFR 1.83(a) because they fail to show element 43 of fig. 4 as described in the specification. These drawings are also objected to under 37 CFR 1.83(a) because they fail to show element 135 as described in lines 1-2 of page 29 of the specification. There are many other instances where elements are referred to in the specification and not in the figures. Consequently, all instances where inconsistencies occurred have not been listed.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "31" (in the figure) and "31'" (in the disclosure) have both been used to designate the modified apparatus. There are many other instances where elements are referred to in the specification as one element and labeled as another element in the figures. Consequently, all instances where inconsistencies occurred have not been listed.

Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for

consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The abstract of the disclosure is objected to because in line 5, reference is made to a database numbered 133 in the figure(s). The numeral reference should be deleted. Correction is required. See MPEP § 608.01(b).

Claim Objections

Claims 8-12 are objected to because of the following informalities:

As per claim 8:

The format used for describing the steps in the method being claimed can be made clearer if the steps are numbered in some form. For example, "security specification hatching step" in line 5 can be preceded with the letter "a" in order to label that step as the initial step of the method. Furthermore, all references to the "security specification hatching step" after that may use the label (in this instance "a") instead of writing out the entire step again, whether the reference is made in this claim or in a latter dependent claim.

As per claim 9:

References to details of the steps originally introduced and defined in the independent claim from which this claim derives need not repeat all of the details. It is sufficient to refer to the step, or the character used to label that step, and then continue to claim further limitations. For example, in lines 4-8, applicants may remove "made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step" because this information has already been clarified in the parent claim. This also occurs in lines 18-22 from "made to correspond..." to "...hatching step."

As per claims 10-12:

These claims are objected to by virtue of their dependency.

The previous suggestions have been made in order to prevent any confusion regarding the claimed invention. Generally, the use of repetition may result in unnecessary confusion as to what is being claimed. Please make appropriate corrections.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 8:

Claim 8 is written/translated in a manner that renders the claim indefinite. In one instance, lines 9-10 mention "an" information security policy, where an information security policy is previously introduced in line 6. It is unclear whether applicants intended to refer to the information security policy that was previously introduced or if they are introducing a new one. It is presumed that the applicants intended to refer to the previously introduced information security policy. Accordingly, "an" in line 9 has been interpreted to be "the." Other aspects rendering the claim unclear have also been interpreted in as follows in order to further treat this claim on its merits:

A security management method for supporting a security management of each of a plurality of managed systems constituting an information system with an electronic computer comprising:

a security specification hatching step of extracting an information security policy, made to correspond to each managed system constituting an information system designated by a user, from a database describing a correspondence of the information security policy representing a policy of a security measure with at least one managed system in order to hatch security specifications to be applied to the information system.

a security diagnosis step of executing a plurality of audit programs describing a process for auditing various information, including a type of the managed system and a software version, stored so as to correspond to each set of the information security policy and the managed system which are specified by security specifications hatched in said security specification hatching step, as well as by a security status to audit the various information including the type and the

software version of the managed system constituting the information system designated by the user, and to diagnose a security of said information system; and

a security handling and management step of executing a management program designated by the user, from a plurality of management programs describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system which are specified by the security specifications hatched in said security specification hatching step, to allow said electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program.

As per claim 9:

Claim 9 is written/translated in a manner that renders the claim indefinite. In one instance, line 12 mentions "a" type and "a" software version, where these elements have been previously introduced in lines 16-17 of the parent claim. It is unclear whether applicants intended to refer to the type and software version that were previously introduced or if they are introducing new ones. It is presumed that the applicants intended to refer to the previously introduced type and software versions. Accordingly, "an" in line 10 has been replaced with "the."

As per claim 10:

This claim is rejected by virtue of its dependency on claim 8.

As per claim 11:

Claim 11 is written/translated in a manner that renders the claim indefinite. In lines 3-4, applicants introduce "a setting content received from the user," where it is unclear what "a setting content" is. Although there are many different ways to interpret the applicants' intent, in order to further treat this claim on its merits, it is presumed that the applicants intended to introduce "a security setting content received from the user."

As per claim 12:

Claim 12 is written/translated in a manner that renders the claim indefinite. In one instance, lines 10-11 mentions "an" audit/management program, where an audit/management program has been previously introduced in lines 15 and 30 of the parent claim. It is unclear whether applicants intended to refer to the audit/management programs that were previously introduced or if they are introducing a new one. It is presumed that the applicants intended to refer to the previously introduced audit/management programs. Accordingly, "an" in line 10 has been interpreted to be "the."

As per claim 13:

Claim 13 is written/translated in a manner that renders the claim indefinite. In one instance, line 8 mentions "an" information security policy, where an information security policy is previously introduced in lines 4-5. It is unclear whether applicants intended to refer to the information security policy that was previously introduced or if they are introducing a new one. It is presumed that the applicants intended to refer to the previously introduced information security policy. Accordingly, "an" in line 8 has been interpreted to be "the."

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 8-11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel United States Patent No. 6,484,261 and further in view of Grimm et al. United States Patent No. 6,317,868.

As per claim 8:

Wiegel substantially teaches the claimed security management method for supporting a security management of each of a plurality of managed systems constituting an information system with an electronic computer, comprising a security specification hatching step of extracting an information security policy made to correspond to each managed system constituting an information system (col. 13, lines 29-37 and fig. 7B, elements 726, 728, and 730) designated by a user (col. 13, lines 38-49) from a database (col. 11, lines 43-47 and col. 14, lines 20-35) describing a correspondence of the information security policy (col. 13, lines 38-49) representing a policy of a security measure with at least one managed system (col. 13, lines 1-9 and 49-56), to hatch security specifications (col. 13, lines 14-20) to be applied to the information system (col. 13, lines 20-22).

Not explicitly disclosed by Wiegel is a security diagnosis step of executing a plurality of audit programs describing a process for auditing various information, including a type of the managed system and a software version, stored so as to correspond to each set of the information

security policy and the managed system which are specified by security specifications hatched in said security specification hatching step, as well as by a security status to audit the various information including the type and the software version of the managed system constituting the information system designated by the user, and to diagnose a security of said information system; and a security handling and management step of executing a management program designated by the user, from a plurality of management programs describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system which are specified by the security specifications hatched in said security specification hatching step, to allow said electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program.

However, Grimm et al. teach a security diagnosis step of executing a plurality of audit programs (fig. 1, elements 11 and 21) describing a process for auditing various information (col. 7, lines 27-34), including a type of the managed system (col. 4, lines 9-34) and a software version (col. 5, lines 16-27), stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by security specifications hatched in said security specification hatching step (as applied with Wiegel above), as well as by a security status to audit the various information including the type and the software version of the managed system (col. 7, lines 27-34) constituting the information system designated by the user (fig. 2, element 10), and to diagnose a security of said information system (fig. 2, element 14 and col. 5, lines 13-39).

Also disclosed by Grimm et al. is a security handling and management step of executing a management program designated by the user, from a plurality of management programs (col. 4, lines 24-34 and fig. 1, element 17) describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by the security specifications hatched in said security specification hatching step (as applied with Wiegel above), to allow said electronic computer to change the security status of the managed system (col. 4, lines 35-61) corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program (col. 5, lines 52-63).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the method disclosed in Wiegel to add a security diagnosis step and a security handling/management step as disclosed by Grimm et al. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so as suggested by Grimm et al. in "enforcing and auditing site-specific security provisions" (col. 1, lines 15-18 and col. 1, line 58 – col. 2, line 29).

As per claim 9:

Wiegel and Grimm et al. substantially teach the security management method as applied to claim 8 above. Furthermore, Grimm et al. substantially teach the method wherein in said security diagnosis step, the audit program made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications

hatched in said security specification hatching step, is extracted (col. 5, lines 13-51) describing a correspondence of the information security policy, the managed system and the audit program describing a processing for auditing various information such as a type and a software version of said managed system as well as the security status concerning said information security policy of said managed system, and executed, to diagnose the security of the information system designated by said user.

Also, Grimm et al. substantially teach in said security handling and management step, the management programs made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step, are extracted (col. 4, lines 24-34) describing a correspondence of the information security policy, the managed system and the management program describing a processing for controlling the security status concerning the security policy, the managed system and said information security policy of a security of said managed system, and the management program designated by the user is extracted among the extracted programs to be executed (col. 4, lines 24-44), to allow the security status of the managed system corresponding to the extracted management program to adjust to the information security policy corresponding to the management program.

Not explicitly disclosed by Wiegel or Grimm et al. are the audit program and the management programs being extracted from a database. However, Wiegel teaches the method wherein the audit program and the management programs, which are used for configuring and maintaining the system, are extracted from a database. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the method

disclosed in Wiegel and Grimm et al. to allow for the audit program and management programs to be extracted from the database. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Wiegel in col. 11, lines 43-51.

As per claim 10:

Wiegel and Grimm et al. substantially teach the security management method as applied in claim 8 above. Not explicitly disclosed by Wiegel or Grimm et al. is the method wherein said security diagnose step is executed periodically. However, Grimm et al. teaches the method wherein said security diagnose step is executed periodically as defined by the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Grimm et al. to allow for the security diagnose step to be executed periodically. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Grimm et al. in col. 5, lines 42-51.

As per claim 11:

Wiegel and Grimm et al. substantially teach the security management method as applied to claim 8. Not explicitly disclosed by Wiegel or Grimm et al. is that method wherein, in accordance with setting a content received from the user, said management program changes the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program. However, Wiegel teaches a security setting content received from the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method

disclosed in Wiegel and Grimm et al. to incorporate a security setting content received from the user in order for the management program to change the security status of the managed system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Wiegel in col. 14, lines 1-61.

As per claim 13:

Wiegel substantially teaches the claimed security management system for supporting a security management of managed systems constituting an information system, comprising a database (col. 11, lines 43-47 and col. 14, lines 20-35) describing a correspondence of an information security policy (col.13, lines 38-49) representing a policy of a security measure with at least one managed system (col. 13, lines 1-9 and 49-56) and a security specification hatching section for extracting an information security policy made to correspond to each of the managed systems constituting the information system (col. 13, lines 29-37 and fig. 7B, elements 726, 728, and 730) designated by a user (col. 13, lines 38-49) from said database (col. 11, lines 43-47 and col. 14, lines 20-35), to hatch security specifications (col. 13, lines 14-20) to be applied to the information system (col. 13, lines 20-22).

Not explicitly disclosed by Wiegel is a plurality of audit sections for auditing various information including a type and a software version of the managed system as well as a security status concerning the information security policy of the managed system, each audit section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching section, a security diagnosis section for diagnosing a security of an

information system designated by said user, on the basis of diagnosis results in each of said audit sections, a plurality of management sections for controlling a security status concerning the information security policy of the managed system, each management section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching step, and a security handling and management section for executing a management section designated by said user, to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.

However, Grimm et al. teach a security management system for supporting a security management of managed systems constituting an information system comprising a plurality of audit sections (fig. 1, elements 11 and 21) for auditing various information (col. 7, lines 27-34), including a type (col. 4, lines 9-34) and a software version of the managed system (col. 5, lines 16-27), as well as a security status concerning the information security policy of the managed system (col. 7, lines 27-34), each audit section being provided so as to correspond to each set of the information security policy and the managed system (col. 7, lines 27-34), which are specified by security specifications hatched by said security specification hatching section (as applied with Wiegel above) and a security diagnosis section for diagnosing a security of an information system designated by said user (fig. 2, element 10), on the basis of diagnosis results in each of said audit sections (col. 5, lines 13-39 and fig. 2, element 14).

Also disclosed by Grimm et al. is a plurality of management sections (col. 4, lines 24-34 and fig. 1, element 17) for controlling a security status concerning the information security

policy of the managed system, each management section being provided so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by security specifications hatched in said security specification hatching step (as applied with Wiegel above) and a security handling and management section for executing a management section designated by said user (col. 4, lines 24-34 and fig. 1, element 17), to change the security status of the managed system (col. 4, lines 35-61) corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program (col. 5, lines 52-63).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the method disclosed in Wiegel to add a security diagnosis step and a security handling/management step as disclosed by Grimm et al. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so as suggested by Grimm et al. in "enforcing and auditing site-specific security provisions" (col. 1, lines 15-18 and col. 1, line 58 – col. 2, line 29).

III. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel United States Patent No. 6,484,261, Grimm et al. United States Patent No. 6,317,868, and further in view of CERT's CC Vendor-Initiated Bulletins 1994-1998.

As per claim 12:

Wiegel and Grimm et al. substantially teach the security management method, wherein a diagnosis results obtained in said security diagnose step which is executed for the information system designated by the user are reflected in the database describing the correspondence of the

information security policy with at least one managed system and an audit/management program stored so as to correspond to each set of the information security policy and the managed system as applied to claim 8 above. Not explicitly disclosed by Wiegel or Grimm et al. is security hole information published by a security information organization including CERT or Computer Emergency Response Team. However, CERT/CC Vendor–Initiated Bulletins disclose security hole information published by a security information organization including CERT. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wiegel and Grimm et al. to incorporate the use of security hole information published by a security information organization including CERT or Computer Emergency Response Team. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the CERT/CC Vendor –Initiated Bulletins 1994-1998, pages 1-8.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Pub. No. 2002/0188861 has been cited as a reference because it is relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2133
11/04/2004

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100